Queen's University Belfast

**TrueCrypt – User Guide**

TrueCrypt is a free open-source disk encryption software for Windows Vista/XP, Mac OS X, and Linux and is available at http://www.truecrypt.org/.

This guide describes the use of TrueCrypt to perform three different encryption tasks:

1 Encrypting a Complete System Disk

2 Creating an encrypted volume in a file container

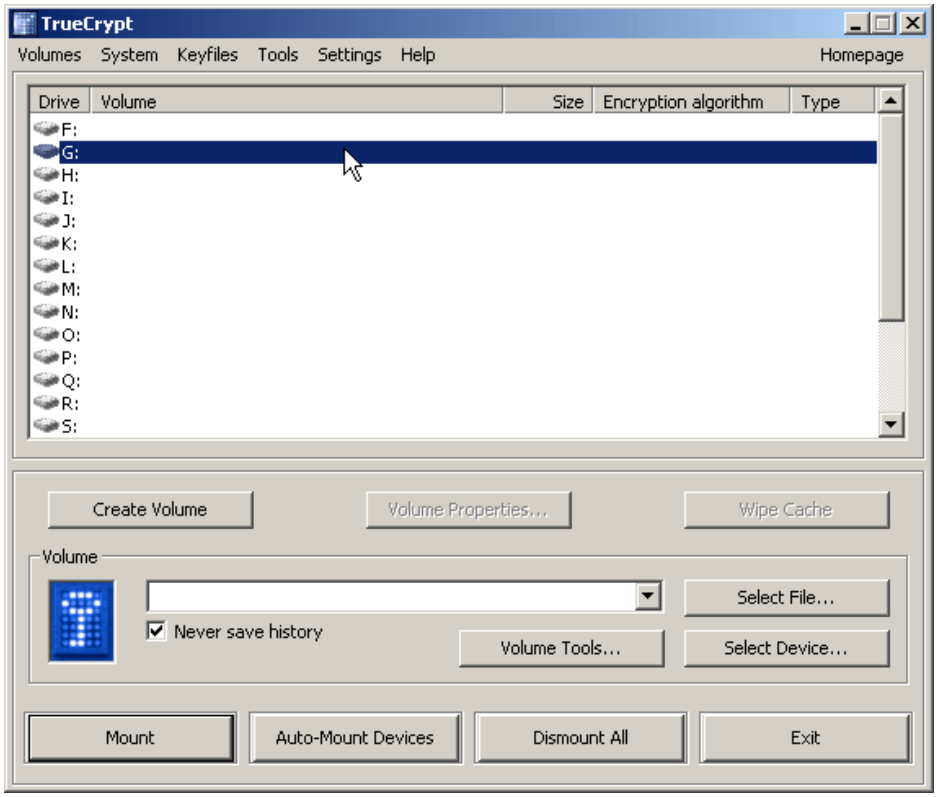
3 Creating an encrypted volume in a non-system partition or device, such as USB memory stick

TrueCrypt 5.1A software was used to perform the encryption tasks. Earlier or later versions may possess a different look and feel, and may offer a different set of functionality.

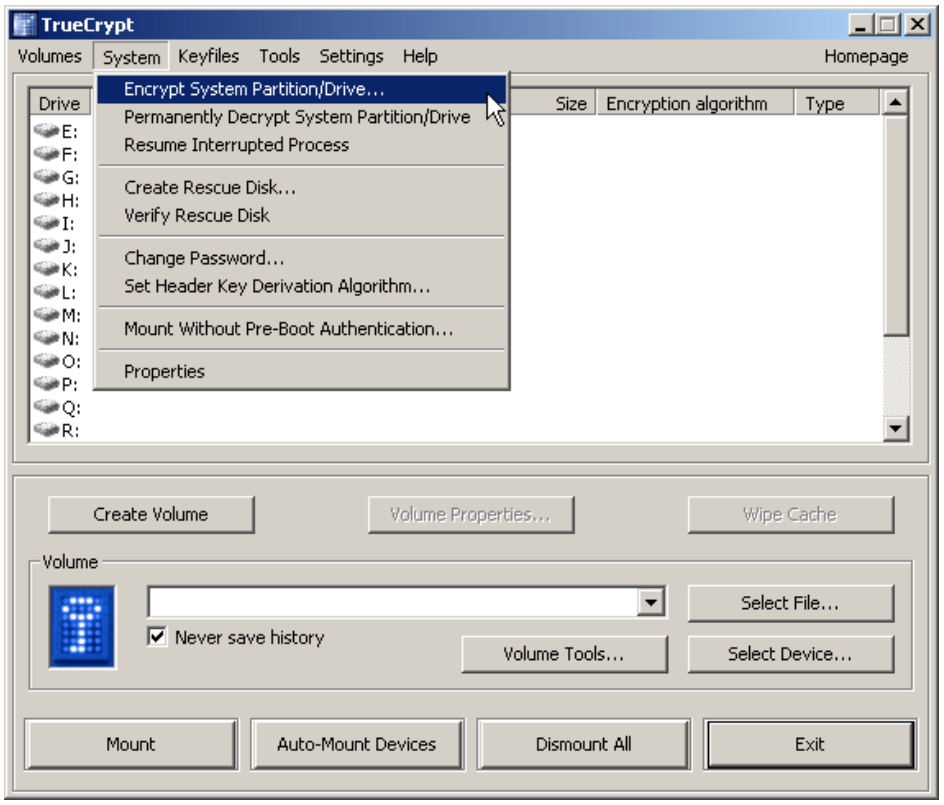
There are quite a few screen shots to display, theretore the document and processes seem long. This is a consequence of offering the user options at various stages of the encryption process and ensuring that it is safe to proceed. In reality, the process does not take long: it is usually just a case of accepting default settings, except in a few instances. The actual encryption process for a system disk takes a lot longer to perform than the initial steps to set the process up.

## 1 Encrypting a Complete System Disk

Once the TrueCrypt program has been installed on a computer, execute the file TruCrypt.exe and a window like this should appear. This is the main TrueCrypt window from which all encryption is controlled. When encrypting a complete system disk, some suitability tests have to be performed and the process ends up being executed in two stages.



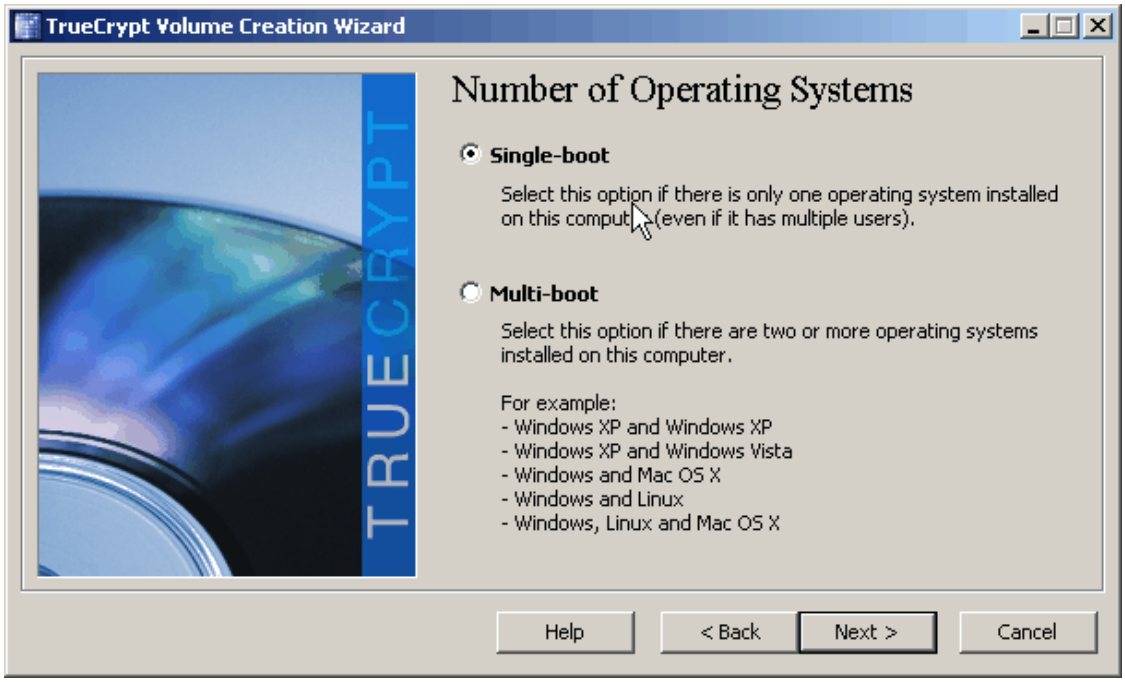

To encrypt a complete system disk, which may contain more than one partition, ensure it contains no logical partitions and click the System option on the menu bar. The menu below will appear. Select the highlighted option.



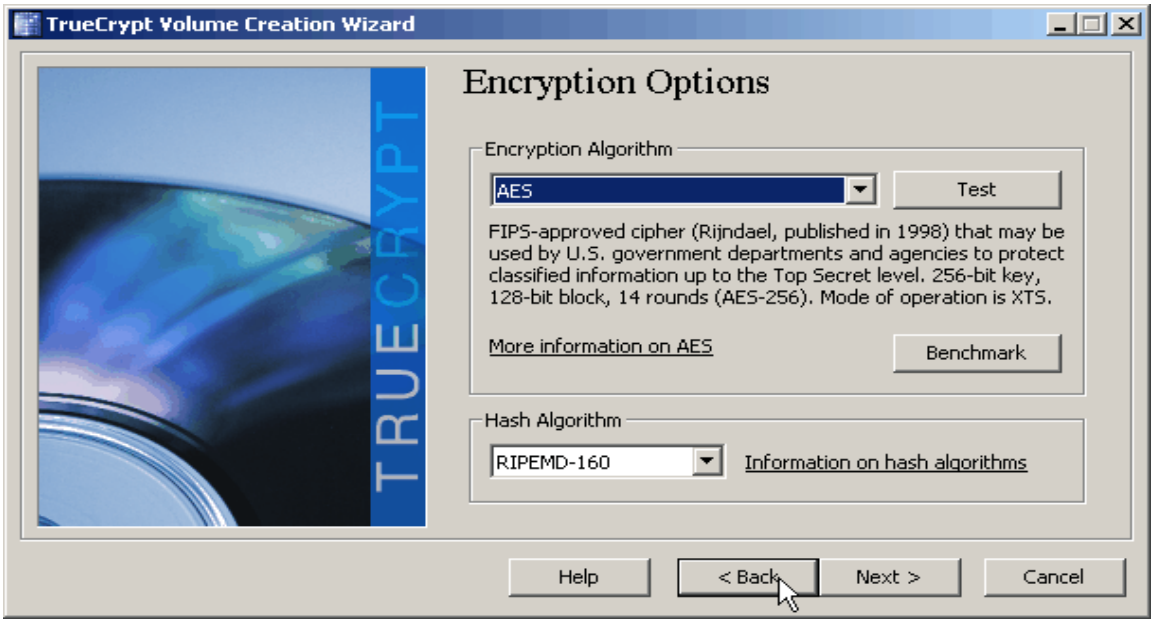

The warning below appears. Click OK if it is safe to proceed.

TrueCrypt Volume Creation Wizard
WARNING: After you start encrypting the drive, you must NOT create any extended (logical) partitions on it (you may create only primary partitions). Any extended partition on the drive would be inaccessible after you start encrypting.
Note: If this limitation is not acceptable, you can go back and choose to encrypt only the system partition instead of the entire drive (and, in addition to that, you can create partition-hosted TrueCrypt volumes within any non-system partitions on the drive).
OK

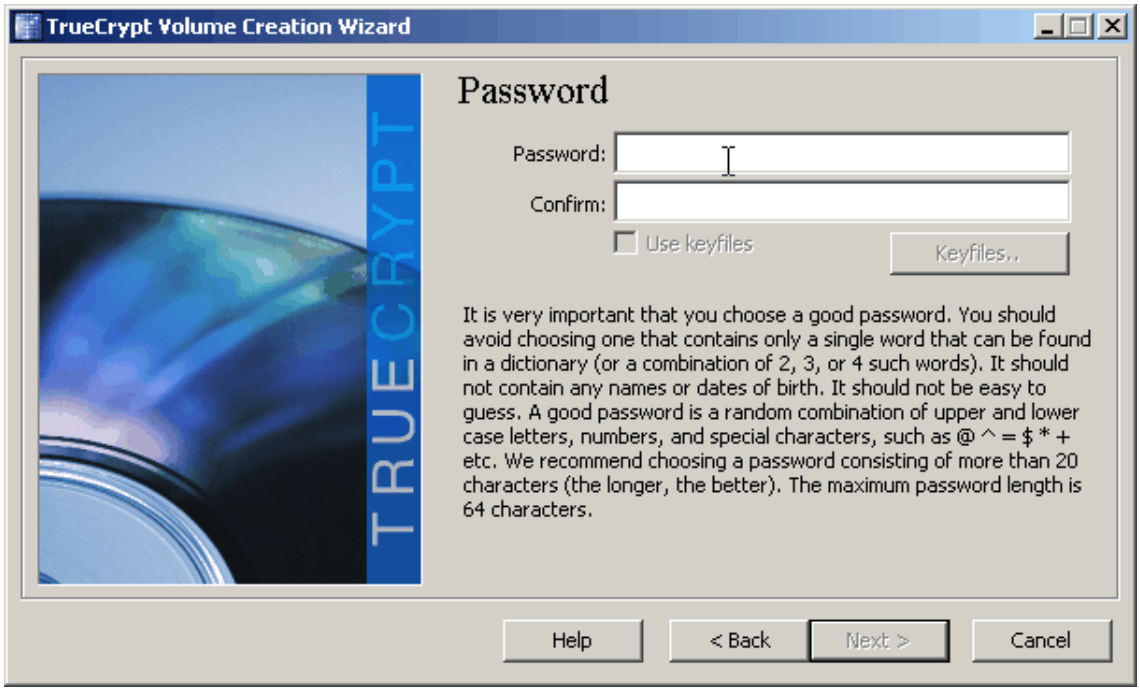
Select the appropriate setting that appears in the next window. In most instances, 'Single-boot' will be the normal selection.


TrueCrypt Volume Creation Wizard
Number of Operating Systems
Single-boot
Select this option if there is only one operating system installed on this computer (even if it has multiple users).
Multi-boot
Select this option if there are two or more operating systems installed on this computer.
For example:
- Windows XP and Windows XP
- Windows XP and Windows Vista
- Windows and Mac OS X
- Windows and Linux
- Windows, Linux and Mac OS X
Help
< Back
Next >
Cancel

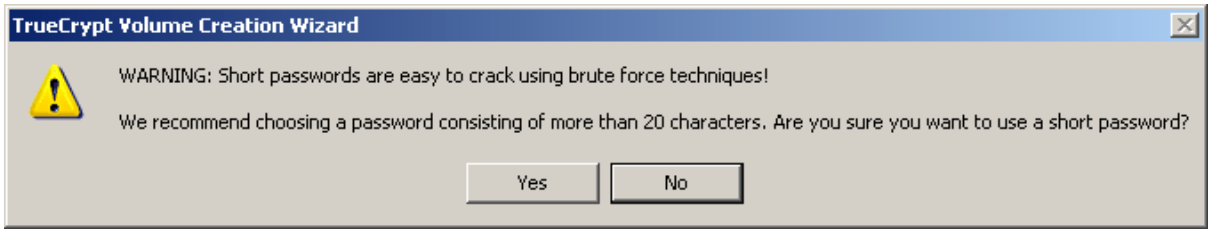
A window presenting encryption options now appears. Unless you know about the meanings of the encryption options and wish to choose differently, accept the default settings.


TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel

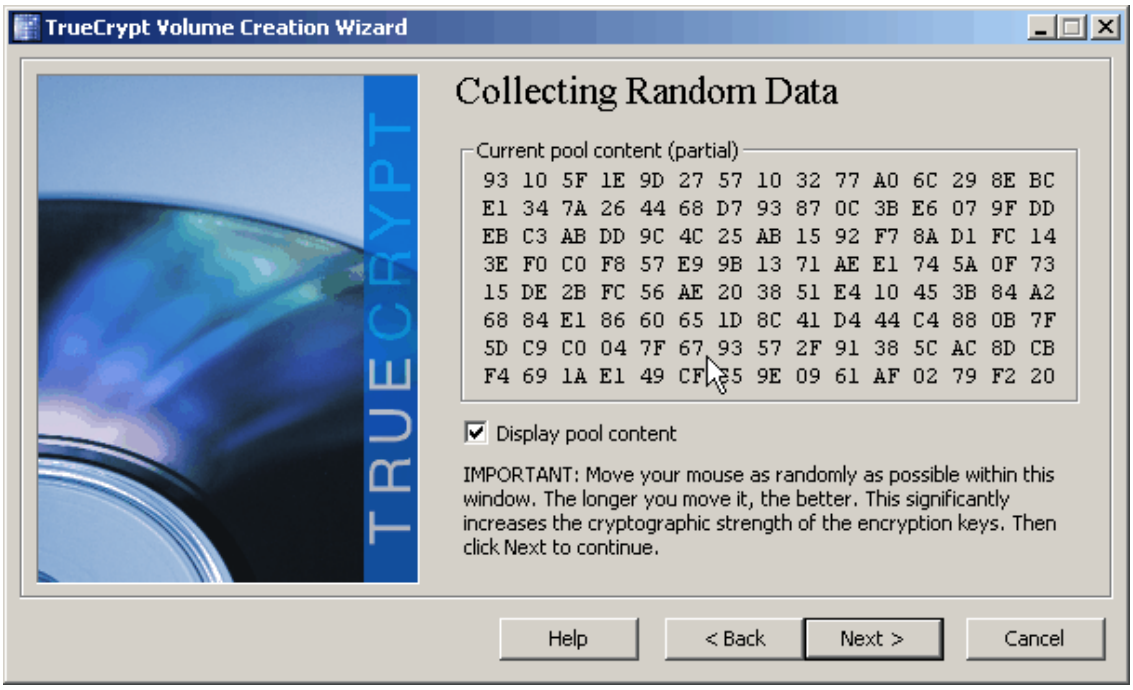
You will now be prompted to type a password. Use a long password or phrase (at least 20 characters is recommended) and make a safe note of it. Loss of this will be catastrophic. Keyfiles can also be specified, which will provide a two-tier level of security, but you must also note the keyfile names.


TrueCrypt Volume Creation Wizard
TRUECRYPT
Password
Password:
Confirm:
Use keyfiles
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.
Help
< Back
Next >
Cancel

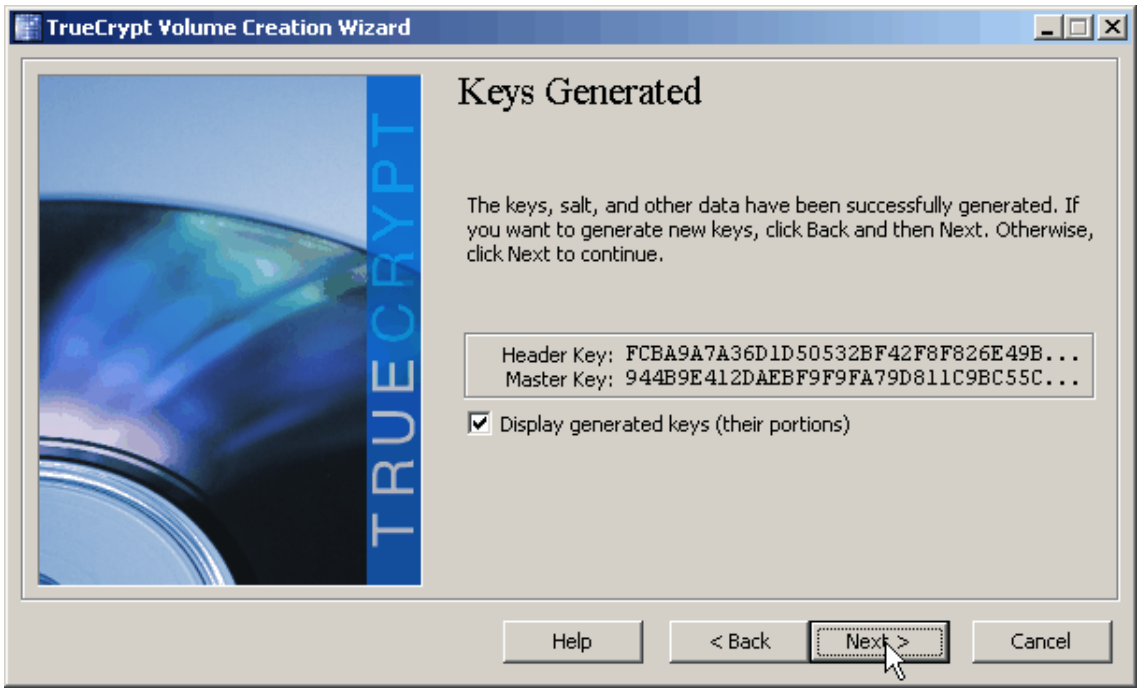
If you type a short password, the warning below will appear and you will be invited to supply another, if you wish.


TrueCrypt Volume Creation Wizard
WARNING: Short passwords are easy to crack using brute force techniques!
We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?
Yes
No

Once a password has been provided, the next window appears. Moving the mouse around within the window for about 30 seconds greatly improves the cryptographic strength of the encryption keys.


TrueCrypt Volume Creation Wizard
Collecting Random Data
Current pool content (partial)
93 10 5F 1E 9D 27 57 10 32 77 A0 6C 29 8E BC
E1 34 7A 26 44 68 D7 93 87 0C 3B E6 07 9F DD
EB C3 AB DD 9C 4C 25 AB 15 92 F7 8A D1 FC 14
3E F0 C0 F8 57 E9 9B 13 71 AE E1 74 5A 0F 73
15 DE 2B FC 56 AE 20 38 51 E4 10 45 3B 84 A2
68 84 E1 86 60 65 1D 8C 41 D4 44 C4 88 0B 7F
5D C9 C0 04 7F 67 93 57 2F 91 38 5C AC 8D CB
F4 69 1A E1 49 CF 25 9E 09 61 AF 02 79 F2 20
Display pool content
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Next to continue.
Help
< Back
Next >
Cancel
TRUECRYPT

TrueCrypt then shows the first few characters of the keys. Click 'Next' to move on to the next stage.


TrueCrypt Volume Creation Wizard
Keys Generated
The keys, salt, and other data have been successfully generated. If you want to generate new keys, click Back and then Next. Otherwise, click Next to continue.
Header Key: FCBA9A7A36D1D50532BF42F8F826E49B...
Master Key: 944B9E412DAEBF9F9FA79D811C9BC55C...
Display generated keys (their portions)
Help
< Back
Next >
Cancel
TRUECRYPT

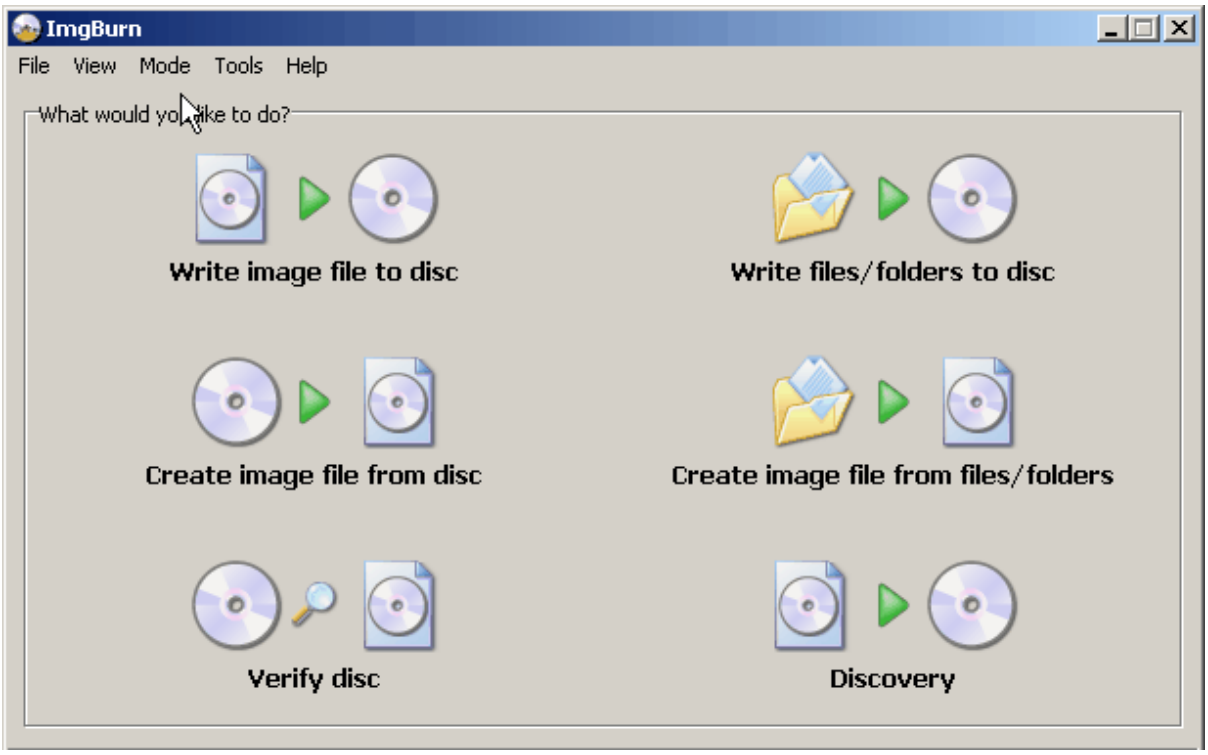
The system now prompts you for a location for the ISO recovery file.

TrueCrypt Volume Creation Wizard
Rescue Disk
Before you can encrypt the partition/drive, you must create a TrueCrypt Rescue Disk (TRD), which serves the following purposes:
- If the TrueCrypt Boot Loader, master key, or other critical data gets damaged, the TRD allows you to restore it (note, however, that you will still have to enter the correct password then).
- If the TrueCrypt Boot Loader gets damaged or infected with malware, you can avoid running it by booting directly from the TRD.
- If Windows gets damaged and cannot start, the TRD allows you to permanently decrypt the partition/drive before Windows starts.
- The TRD will contain a backup of the present content of the first drive cylinder (which typically contains a system loader or boot manager) and will allow you to restore it if necessary.
D:\\TrueCrypt Rescue Disk.iso
Browse...
Help
< Back
Next >
Cancel
TRUECRYPT

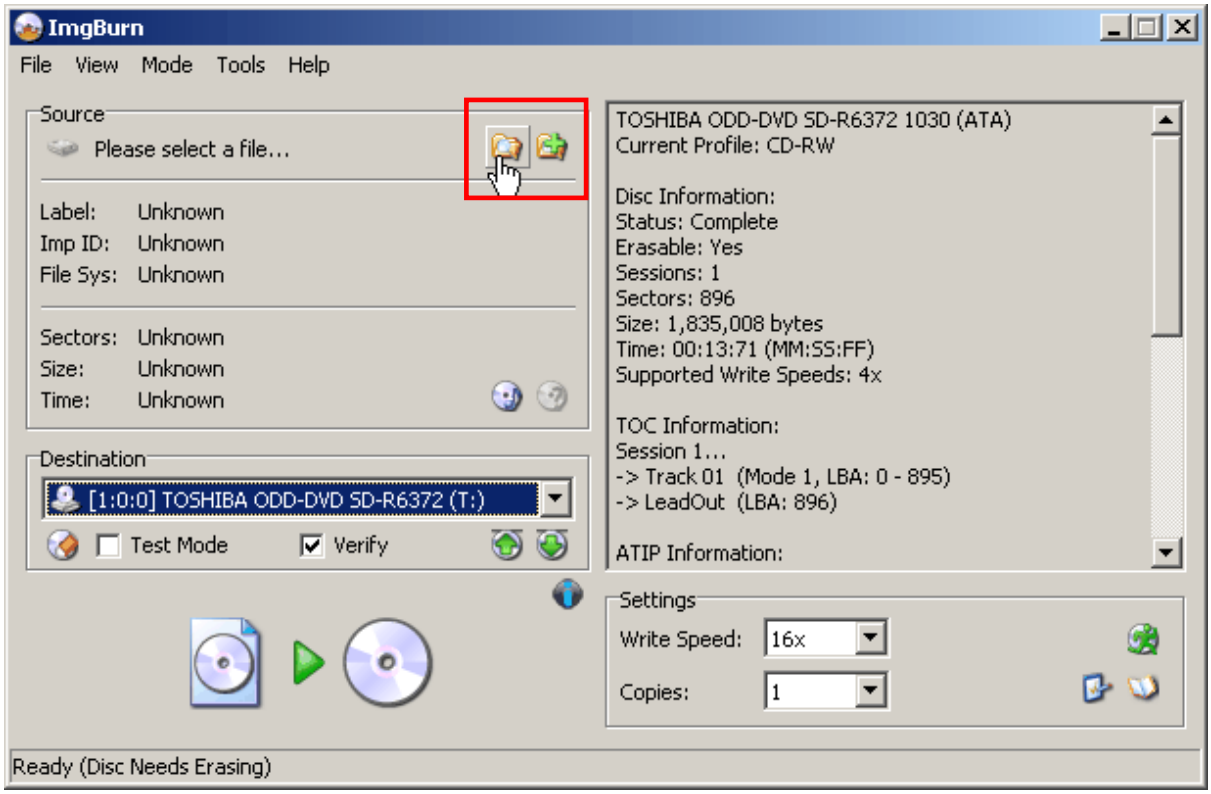
Click 'Next' and an ISO file for the rescue disk will be created. The next window then appears. You must burn the ISO file to a CD or DVD. If you have CD or DVD writer software, use it to do so. If not, you can download the software specified in the link within the window, or use another free package called ImgBurn. Normally, CD or DVD writer software has a facility to write an ISO file to a CD or DVD. An ISO file is just an image to be copied to the output media, so its contents do not need to be known or understood.

TrueCrypt Volume Creation Wizard
Rescue Disk Recording
The Rescue Disk image has been created and stored in this file:
D:\\TrueCrypt Rescue Disk.iso
Now you need to write (burn) the Rescue Disk to a CD or DVD.
IMPORTANT: Note that the file must be written to the CD/DVD as an ISO disk image (not as an individual file). For information on how to do so, please refer to the documentation of your CD/DVD recording software. If you do not have any CD/DVD recording software that can write the ISO disk image to a CD/DVD, click the link below to download such free software.
After you burn the Rescue Disk, click Next to verify that the Rescue Disk has been correctly burned.
Download CD/DVD recording software
Help
< Back
Next >
Cancel
TRUECRYPT

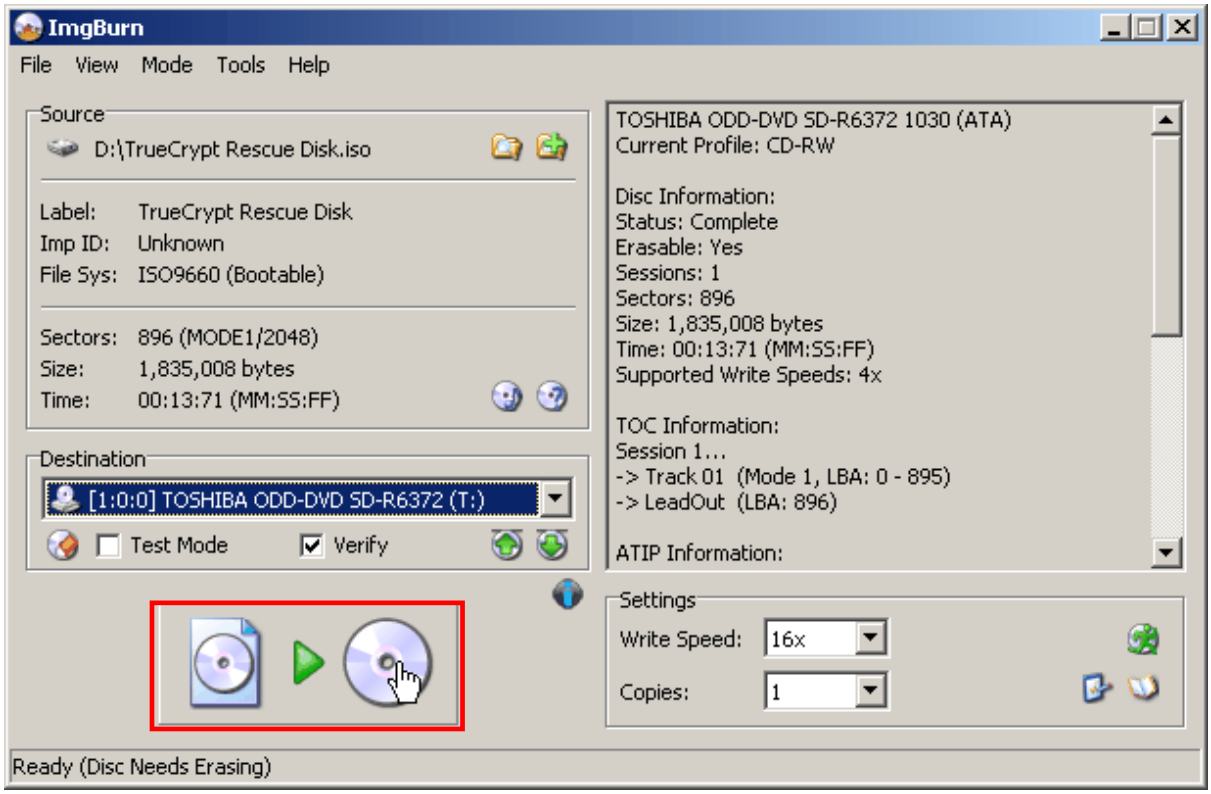
The window following is of ImgBurn in EZ-Mode Picker mode. Simply click on the 'Write image file to disk' option to start the process.




When the next window appears, click on the file selection button (where the hand is inside the red box) and navigate to the ISO rescue file that TrueCrypt has just produced.




In the next window, click on the image at the bottom, within the red box, and the disk burning process will commence. If a re-writable disk is being used, it will have to be erased if it contains data, or formatted if this is its first use. Formatting a DVD takes many minutes, whereas formatting a CD takes a few minutes.

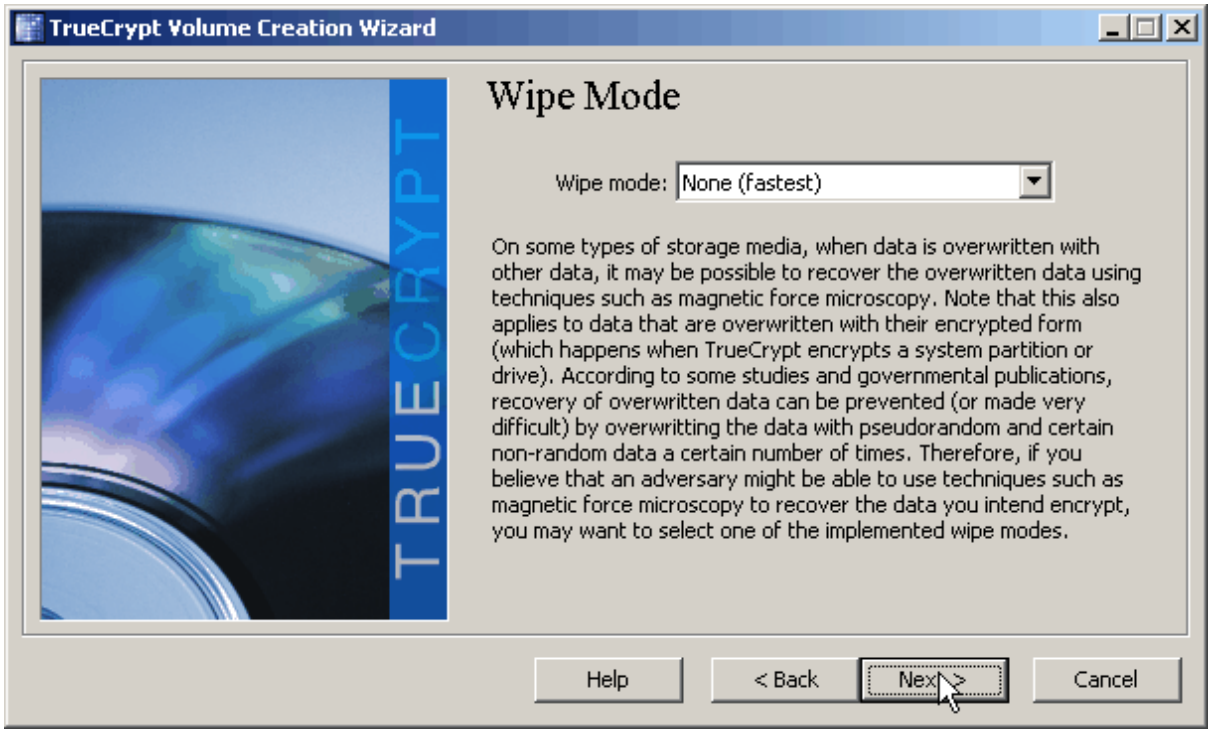



When the rescue disk has been burned, click the 'Next' button on the Rescue Disk Recording window. The next window appears, verifying the successful creation of the rescue disk. Carefully remove the disk, label it and store it away for future use.

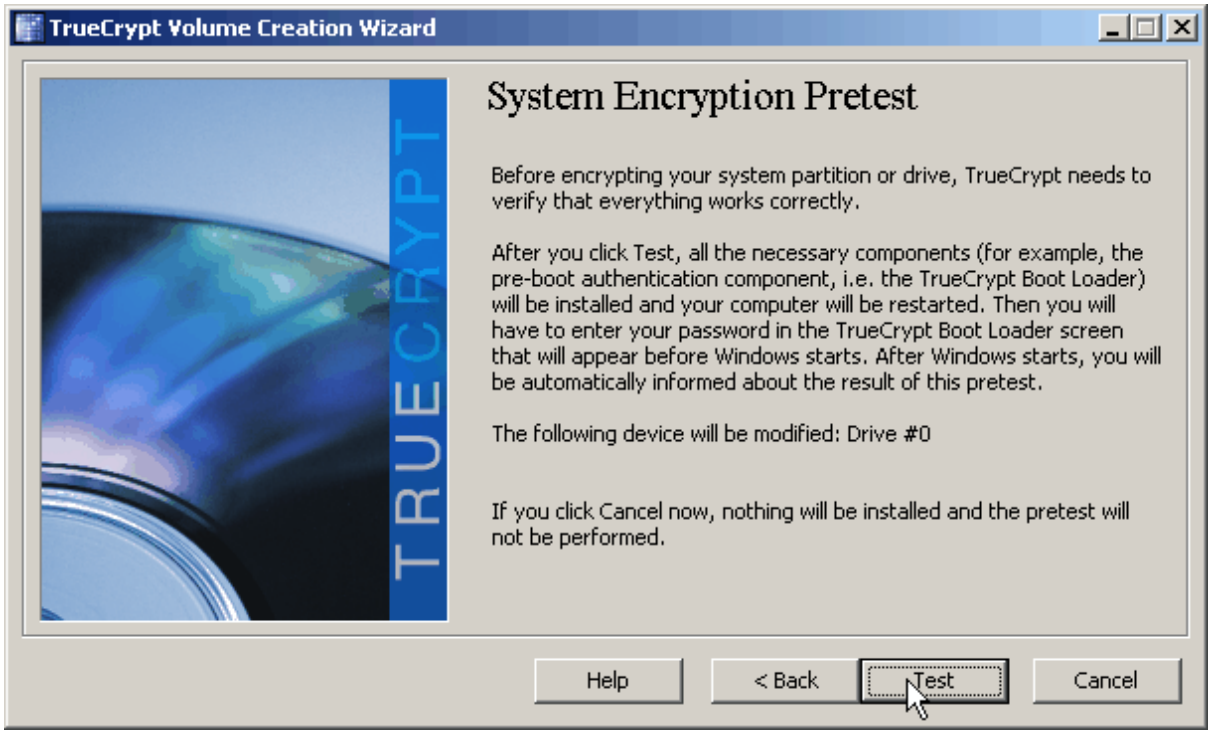
TrueCrypt Volume Creation Wizard
TRUECRYPT
Rescue Disk Verified
The TrueCrypt Rescue Disk has been successfully verified. Please remove it from the drive now and store it in a safe place.
Click Next to continue.
Help
< Back
Next >
Cancel

Clicking 'Next' will cause the next window to appear. If you think someone may be able to recover data from previously used portions of the disk, select a method to obliterate the data on such

partitions, otherwise accept the default value. The default value will be much quicker, but you must assess the chances of data being recovered, as explained in the window.

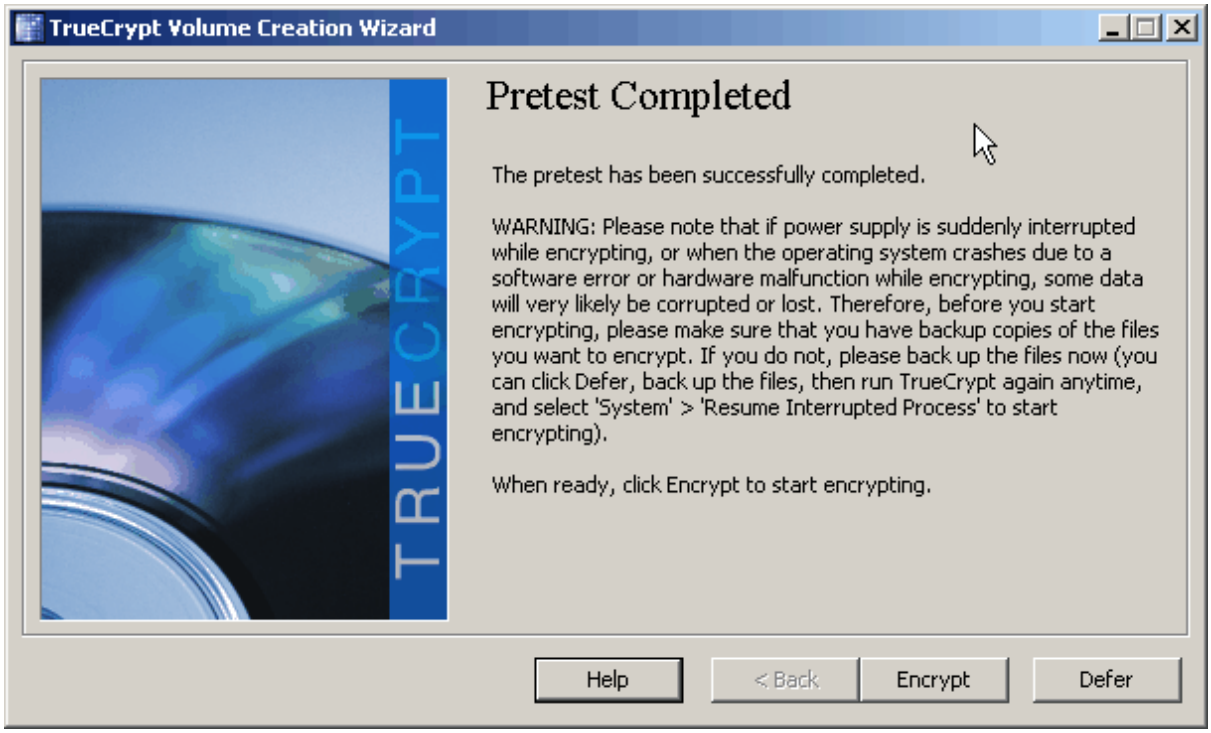

TrueCrypt Volume Creation Wizard
Wipe Mode
Wipe mode: None (fastest)
On some types of storage media, when data is overwritten with other data, it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. Note that this also applies to data that are overwritten with their encrypted form (which happens when TrueCrypt encrypts a system partition or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwritting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use techniques such as magnetic force microscopy to recover the data you intend encrypt, you may want to select one of the implemented wipe modes.
TRUECRYPT
Help
< Back
Next >
Cancel

TrueCrypt is now ready to perform a number of system tests. Click the 'Test' button on the next window.

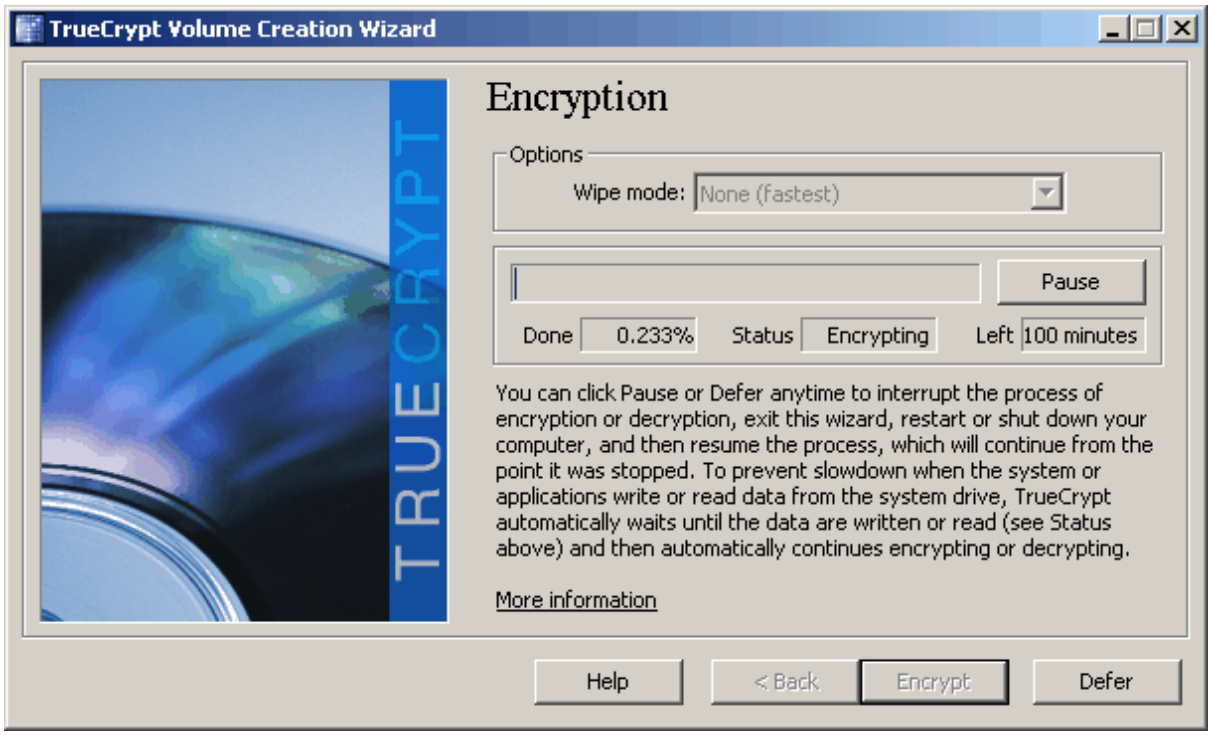

TrueCrypt Volume Creation Wizard
System Encryption Pretest
Before encrypting your system partition or drive, TrueCrypt needs to verify that everything works correctly.
After you click Test, all the necessary components (for example, the pre-boot authentication component, i.e. the TrueCrypt Boot Loader) will be installed and your computer will be restarted. Then you will have to enter your password in the TrueCrypt Boot Loader screen that will appear before Windows starts. After Windows starts, you will be automatically informed about the result of this pretest.
The following device will be modified: Drive #0
If you click Cancel now, nothing will be installed and the pretest will not be performed.
TRUECRYPT
Help
< Back
Test
Cancel

After the pre-test completes, the computer restarts. You will now see the TrueType pre-boot window, at which the TrueType password you set must be given to proceed. The other options should be ignored.

When the system reboots, the next screen appears.


TrueCrypt Volume Creation Wizard
TRUECRYPT
Pretest Completed
The pretest has been successfully completed.
WARNING: Please note that if power supply is suddenly interrupted while encrypting, or when the operating system crashes due to a software error or hardware malfunction while encrypting, some data will very likely be corrupted or lost. Therefore, before you start encrypting, please make sure that you have backup copies of the files you want to encrypt. If you do not, please back up the files now (you can click Defer, back up the files, then run TrueCrypt again anytime, and select 'System' > 'Resume Interrupted Process' to start encrypting).
When ready, click Encrypt to start encrypting.
Help
< Back
Encrypt
Defer

Carefully read the warning message and then, if it is safe to proceed, click the 'Encrypt' button. Shortly after that the next window should appear.


TrueCrypt Volume Creation Wizard
TRUECRYPT
Encryption
Options
Wipe mode: None (fastest)
Pause
Done 0.233% Status Encrypting Left 100 minutes
You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, TrueCrypt automatically waits until the data are written or read (see Status above) and then automatically continues encrypting or decrypting.
More information
Help
< Back
Encrypt
Defer

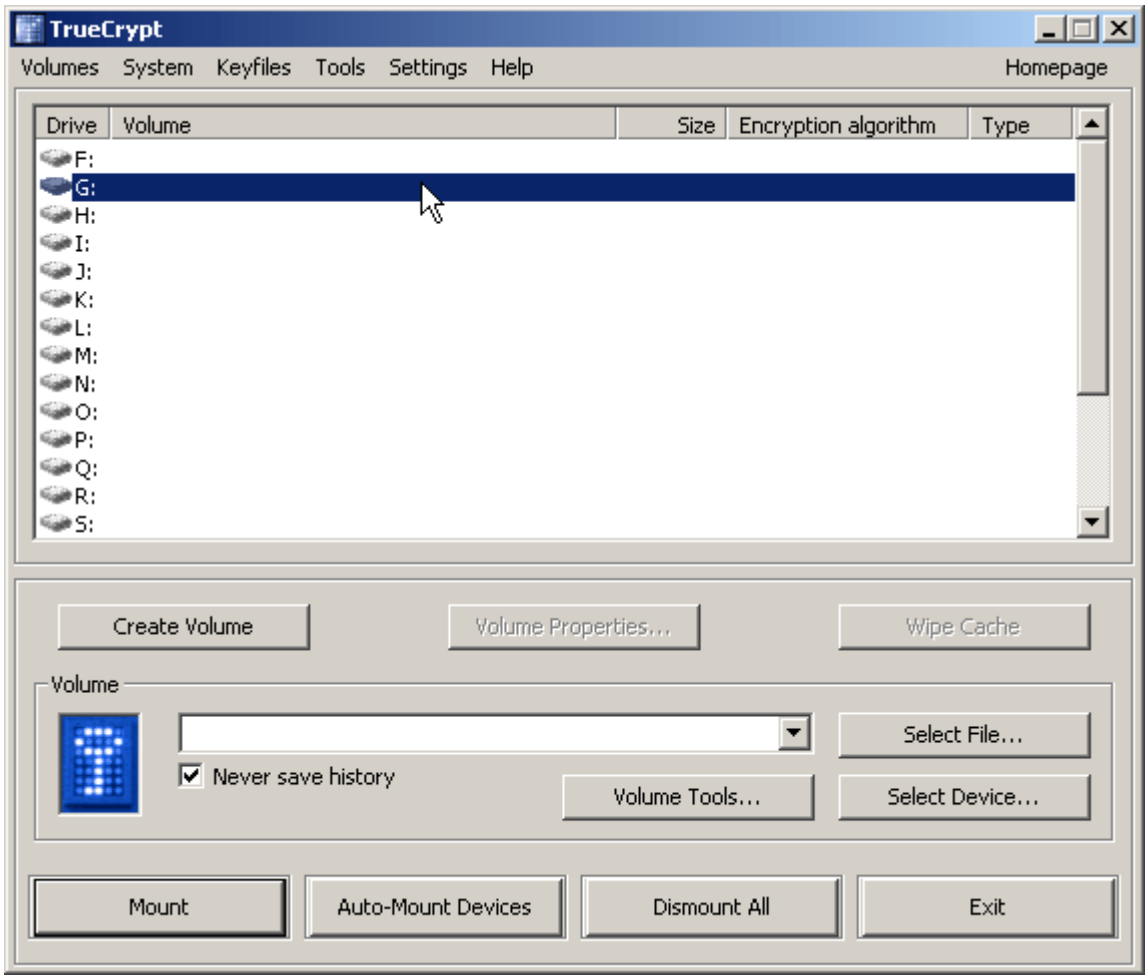
From the text within the window you will see how to interrupt the encryption process if necessary. Depending on the size of the disk, the power of the computer and the options selected, encryption can take several hours to complete. The window shows, graphically and numerically, the progress of the encryption process.

## 2 Create a Virtual Volume Within a File Container

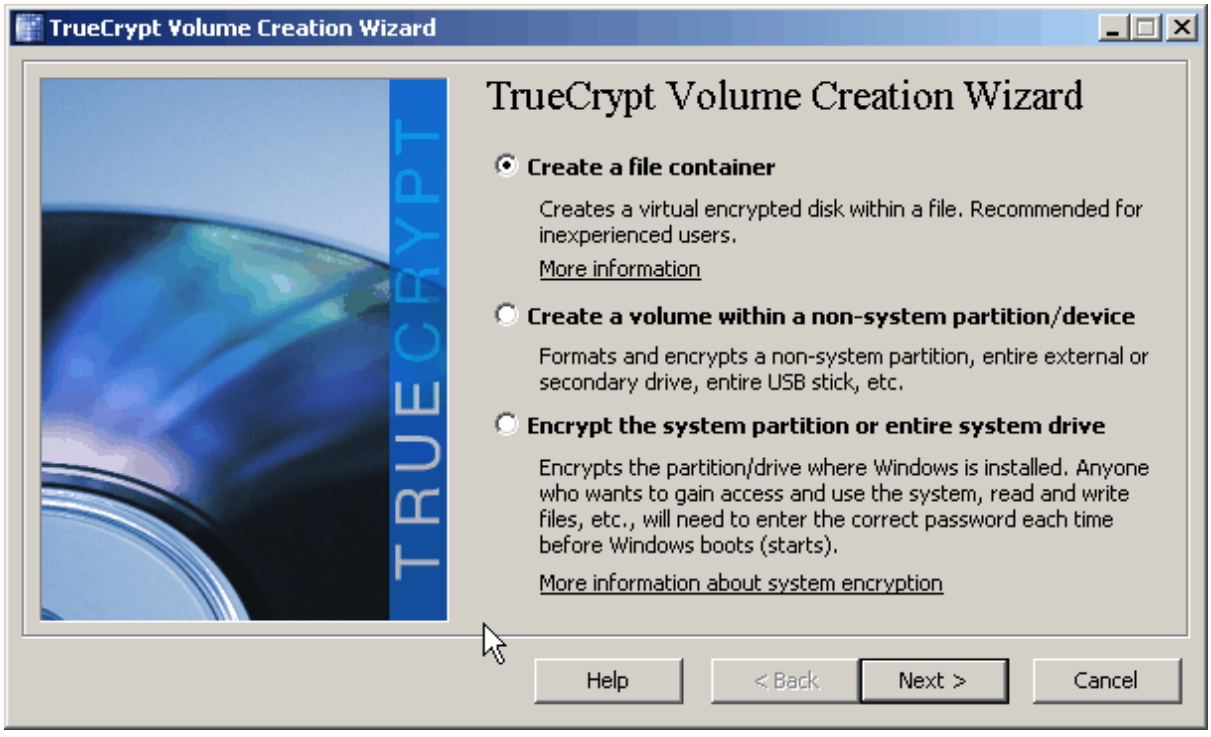
This section shows the steps in creating a virtual volume that is contained within an ordinary-looking file created for the purpose. This is called a file container. If an existing file is used, any data in an existing file will be lost. To retain the file data, rename the file, use the original name to create a new file and, when the virtual volume has been created and mounted, copy the original file into it and it will be encrypted.

Carefully read the text in each window that appears, before clicking the 'Next' button.

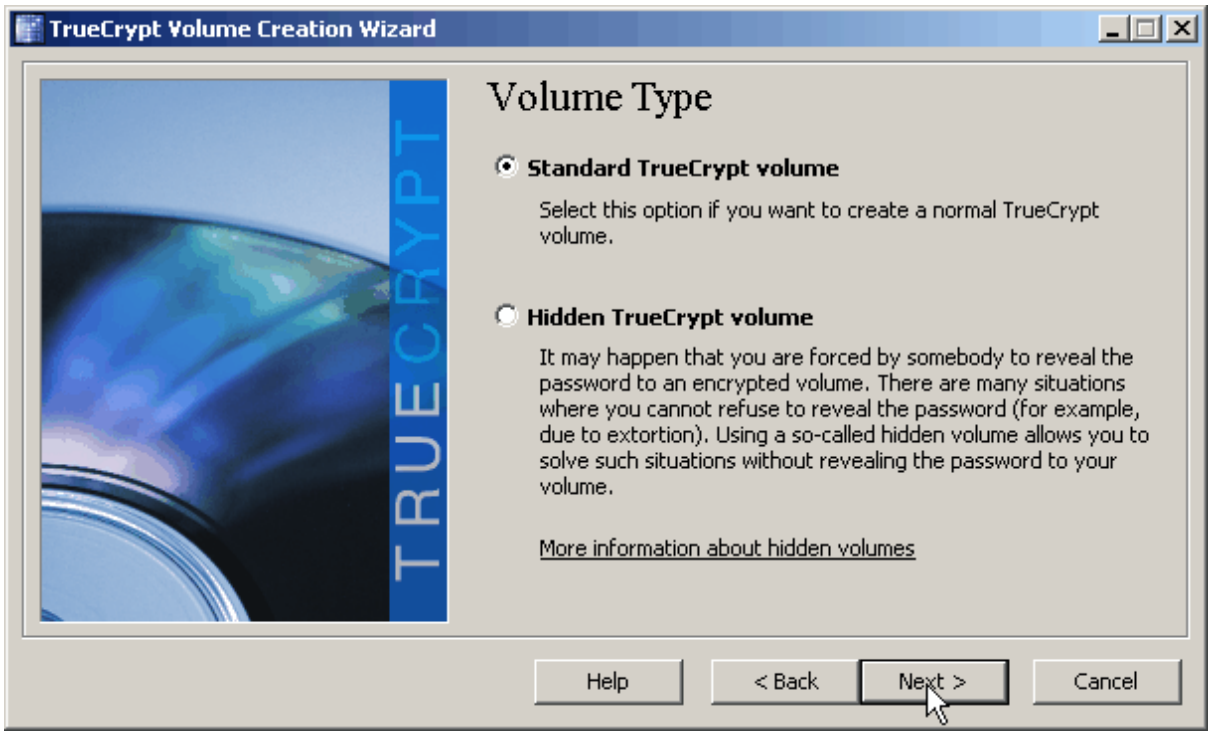
When you start the TrueCrypt application the next window will appear.



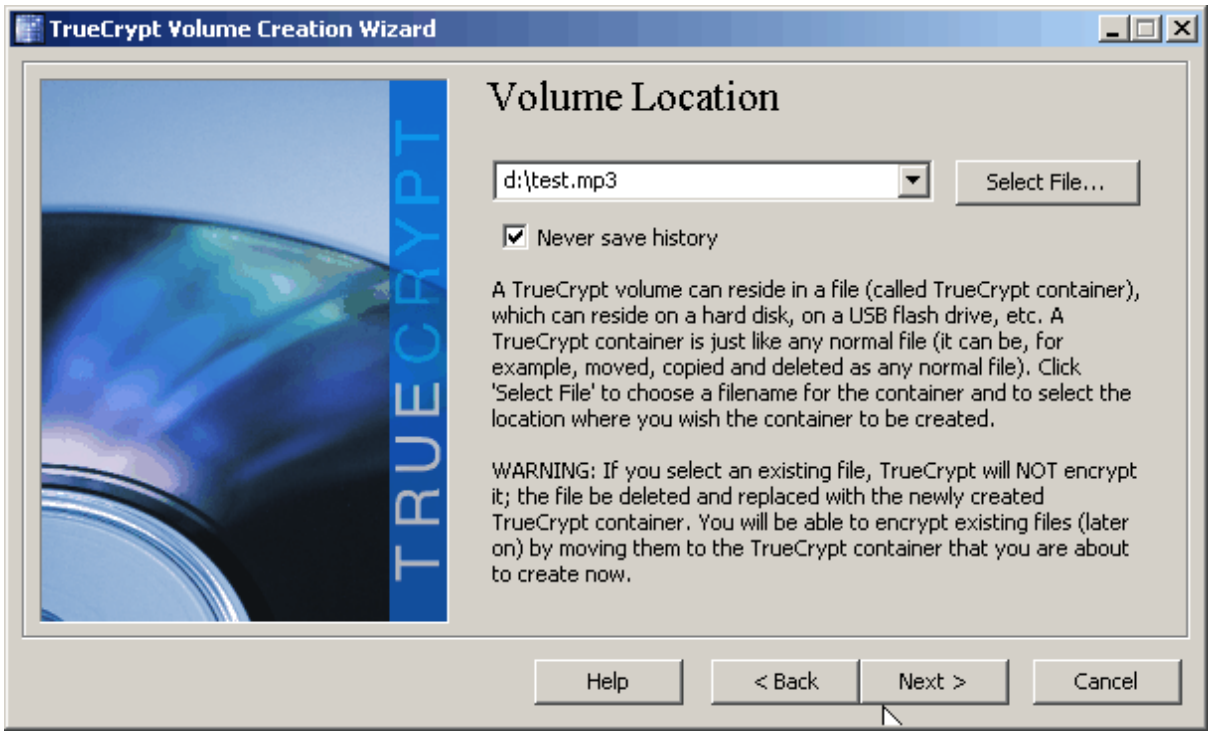

Click the 'Create Volume' button to reach the next window.


TrueCrypt Volume Creation Wizard
TRUECRYPT
TrueCrypt Volume Creation Wizard
Create a file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Create a volume within a non-system partition/device
Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots (starts).
More information about system encryption
Help
< Back
Next >
Cancel

Select the 'Create a file container' option and click 'Next' to move to the next window.


TrueCrypt Volume Creation Wizard
Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
TRUECRYPT
Help
< Back
Next >
Cancel

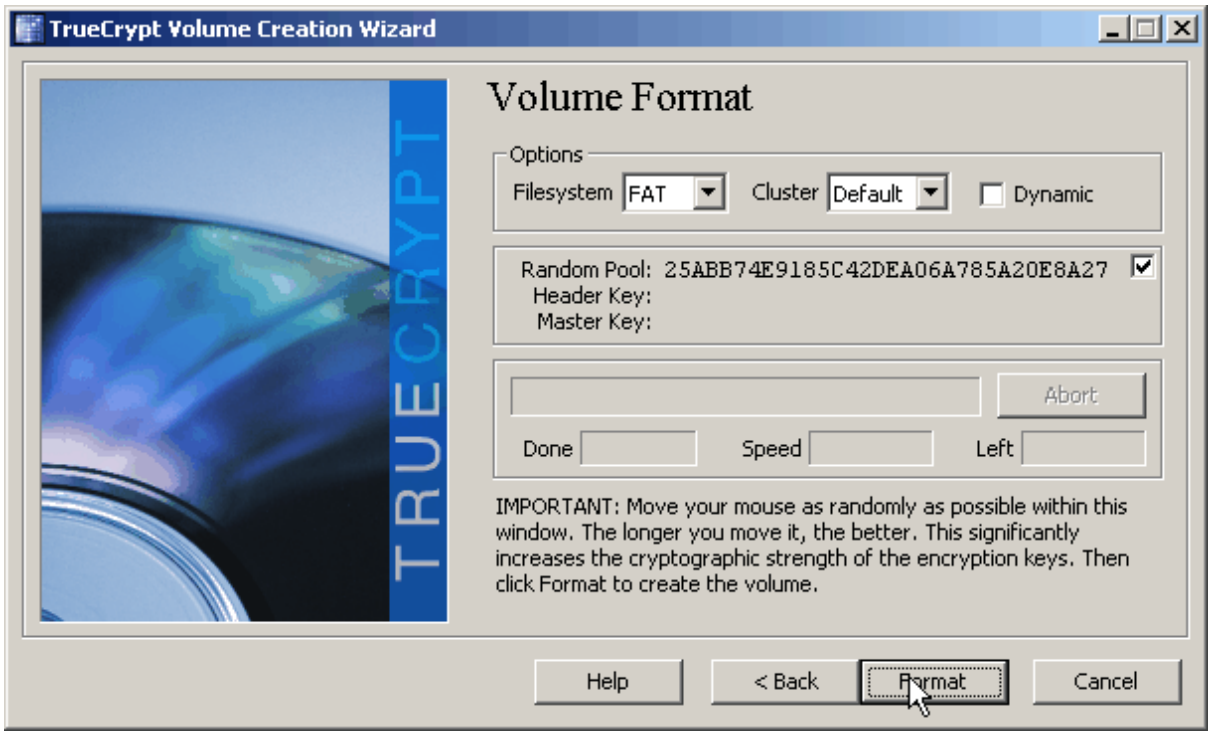
Select the 'Standard TrueCrypt volume' option and click 'Next'.


TrueCrypt Volume Creation Wizard
Volume Location
d:\test.mp3
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
TRUECRYPT
Help
< Back
Next >
Cancel

Type the name of the file to hold the volume. An existing file will lose all its data. Click 'Next'.

TrueCrypt Volume Creation Wizard
Volume Size
1
KB
MB
Free space on drive d:\ is 7332.29 MB.
Please specify the size of the container to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.
Note that the minimum possible size of a FAT volume is 19 KB. The minimum possible size of an NTFS volume is 2573 KB.
TRUECRYPT
Help
< Back
Next >
Cancel

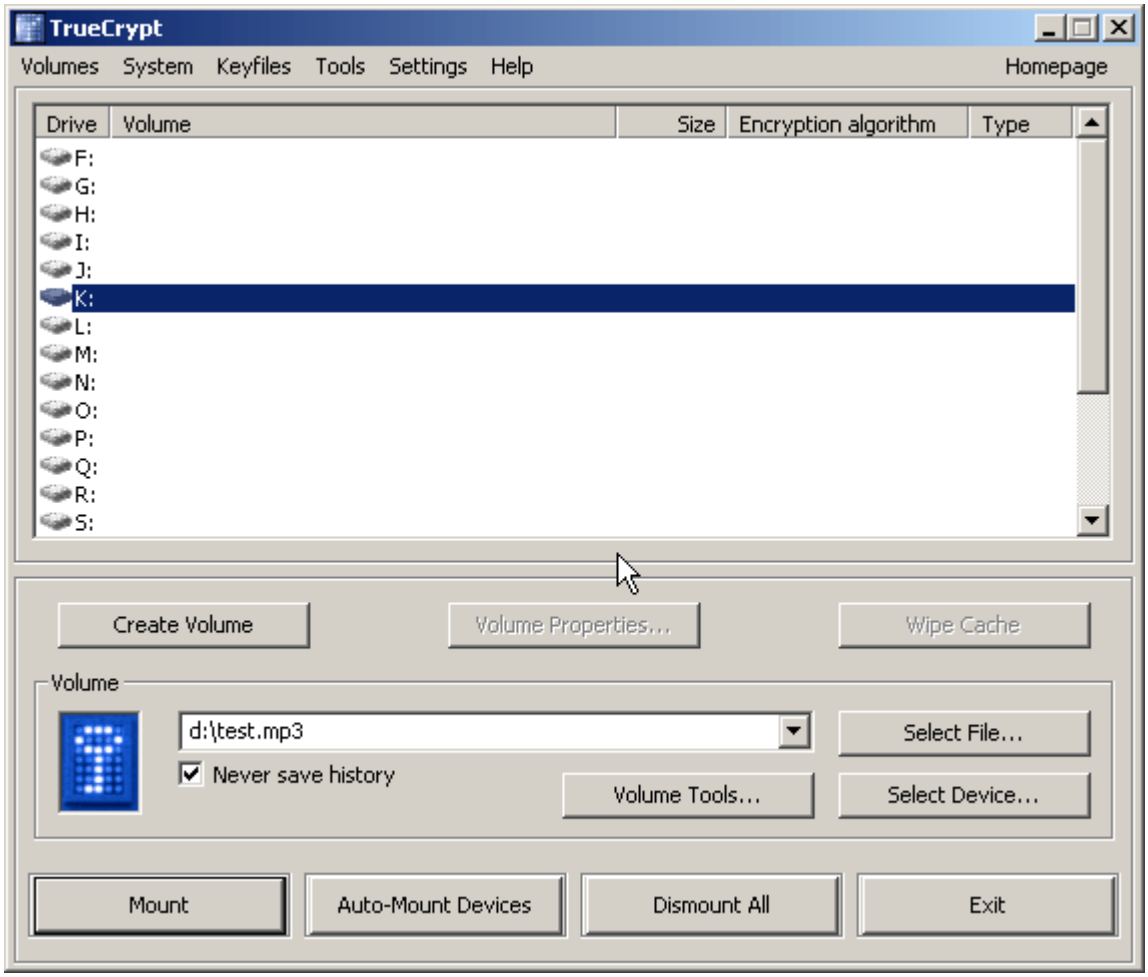
Now provide the size for the new virtual volume and click 'Next'.




Select the filesystem type (normally NTFS) and move the mouse within the window for about 30 seconds, to generate strong cryptographic keys. Click 'Format'. When the process completes, which normally takes a matter of seconds for a small volume, the volume can then be mounted for use.

In the standard TrueCrypt Window, select an unused drive letter, enter the path to the file containing the virtual volume and click the 'Mount' button (see next window). A volume using that drive letter will now be available to store encrypted files. When finished with the volume, select its drive letter and the 'Mount' button will become a 'Dismount' button. Click it to release the volume.

No longer is it possible to use the volume. To all intents and purposes, it is now simply another file, until it is mounted as a volume again.

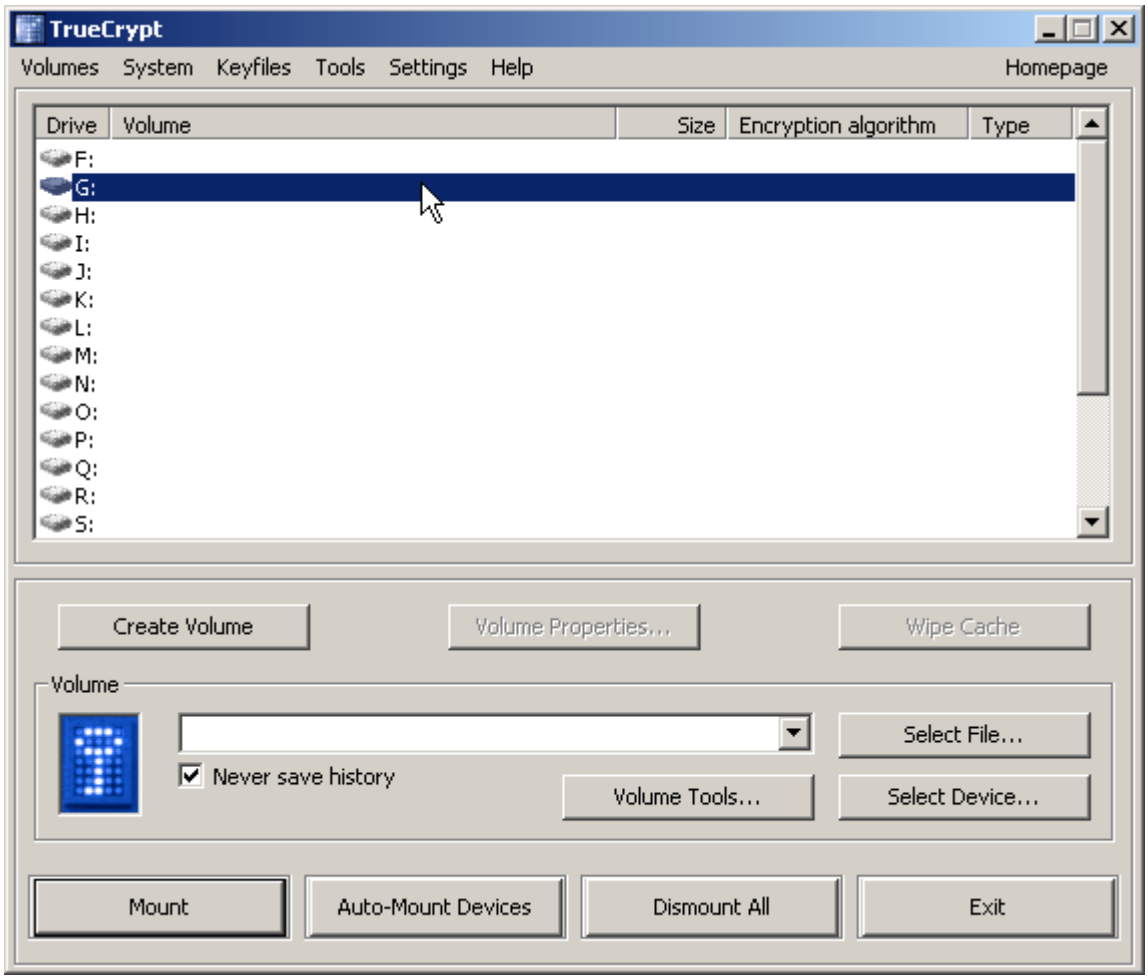



## 3 Create a Virtual Volume Within a Partition

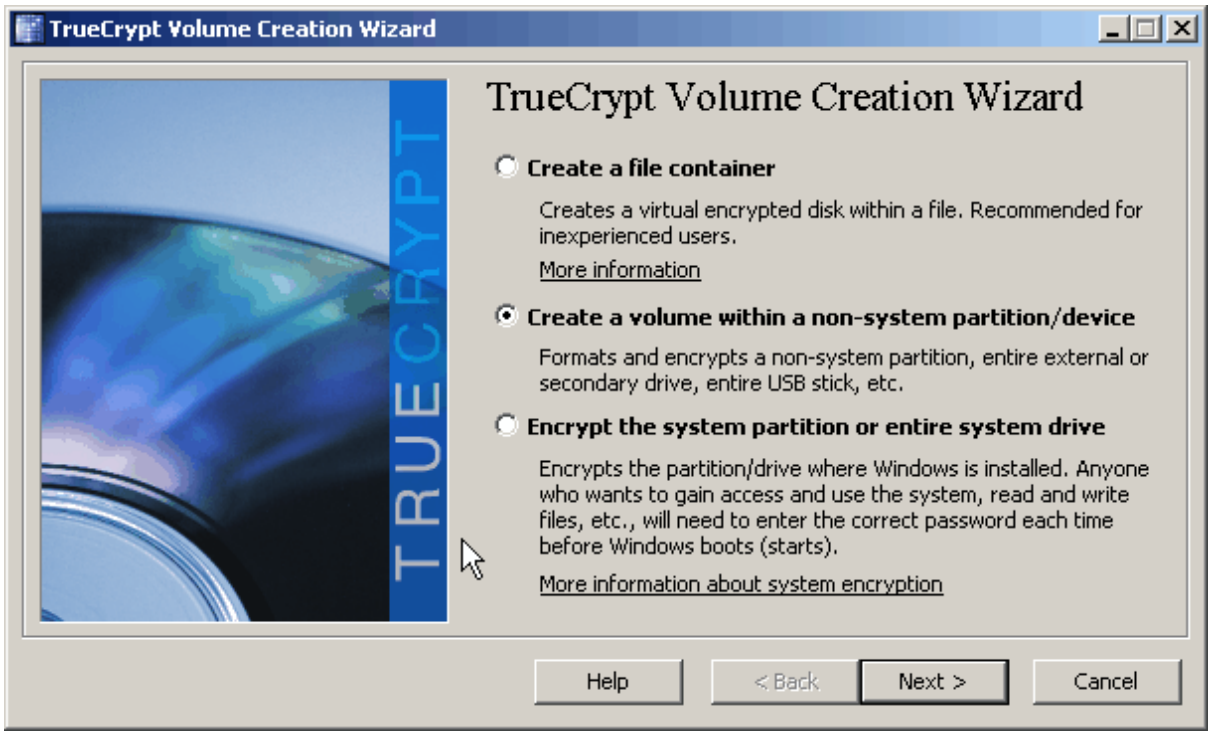
The only time that TrueCrypt encrypts the data in an existing partition is when the system partition is encrypted or when the disk containing the system partition is encrypted. For all other partitions, whether on hard disk, USB disk or USB memory stick, the partition will be formatted when created, thereby overwriting any data. If a partition to be encrypted contains data for retention, it must be copied somewhere else before encrypting the partition, and then copied back to the encrypted partition.

In this example, a USB memory stick will be encrypted, but it could equally well be a partition on a hard disk that is not the system disk.

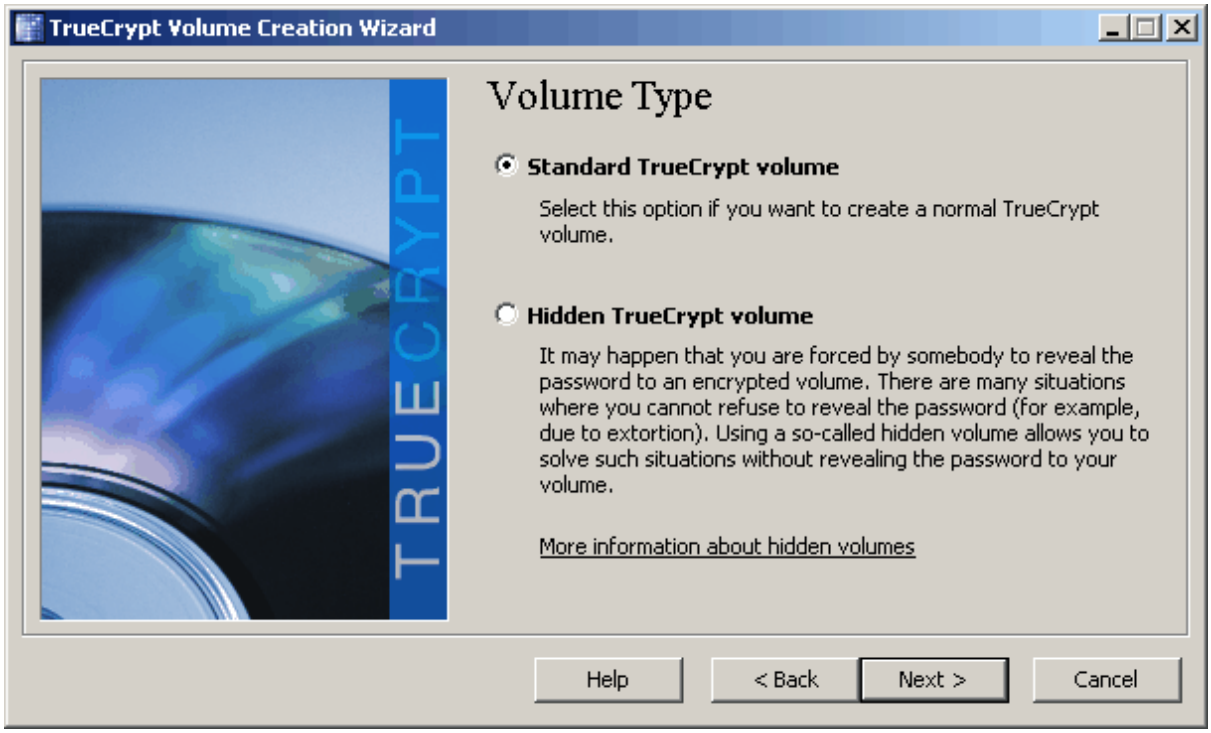
Start TrueCrypt, as before, to bring up the TrueCrypt main window.



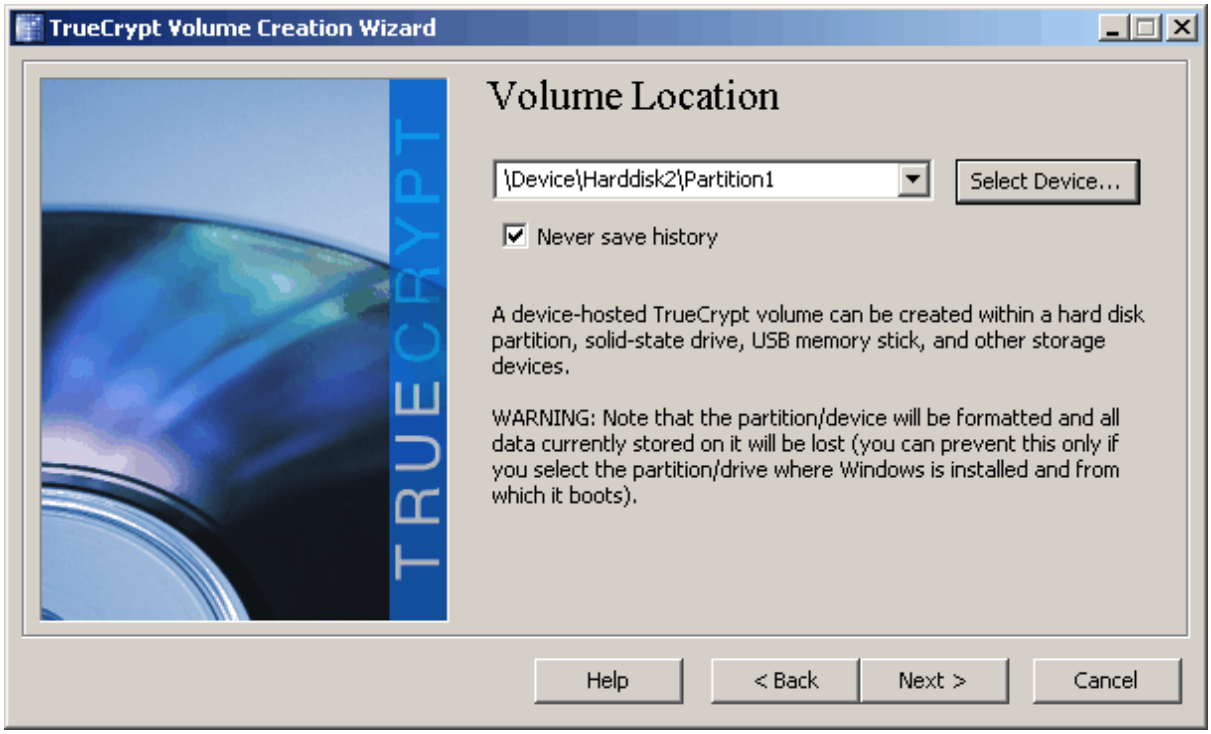

Click the 'Create Volume' button to start the volume creation process. The next window should appear.


TrueCrypt Volume Creation Wizard
TRUECRYPT
TrueCrypt Volume Creation Wizard
Create a file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Create a volume within a non-system partition/device
Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots (starts).
More information about system encryption
Help
< Back
Next >
Cancel

Select the 'Create a volume within a non-system partition/device' option and click 'Next'. The following window appears.


TrueCrypt Volume Creation Wizard
Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
TRUECRYPT
Help
< Back
Next >
Cancel

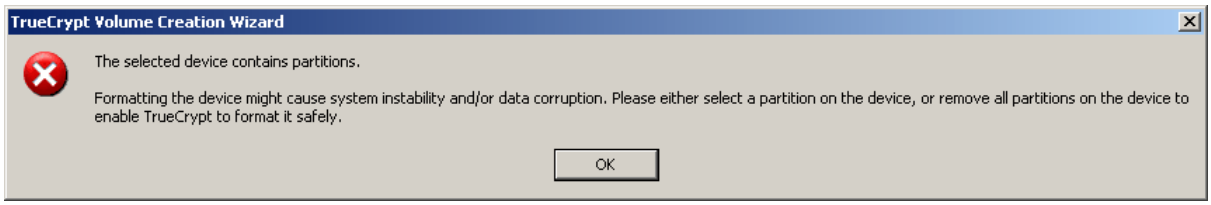
Select the 'Standard TrueCrypt volume' option and click 'Next'.


TrueCrypt Volume Creation Wizard
Volume Location
\Device\Harddisk2\Partition1
Select Device...
Never save history
A device-hosted TrueCrypt volume can be created within a hard disk partition, solid-state drive, USB memory stick, and other storage devices.
WARNING: Note that the partition/device will be formatted and all data currently stored on it will be lost (you can prevent this only if you select the partition/drive where Windows is installed and from which it boots).
TRUECRYPT
Help
< Back
Next >
Cancel

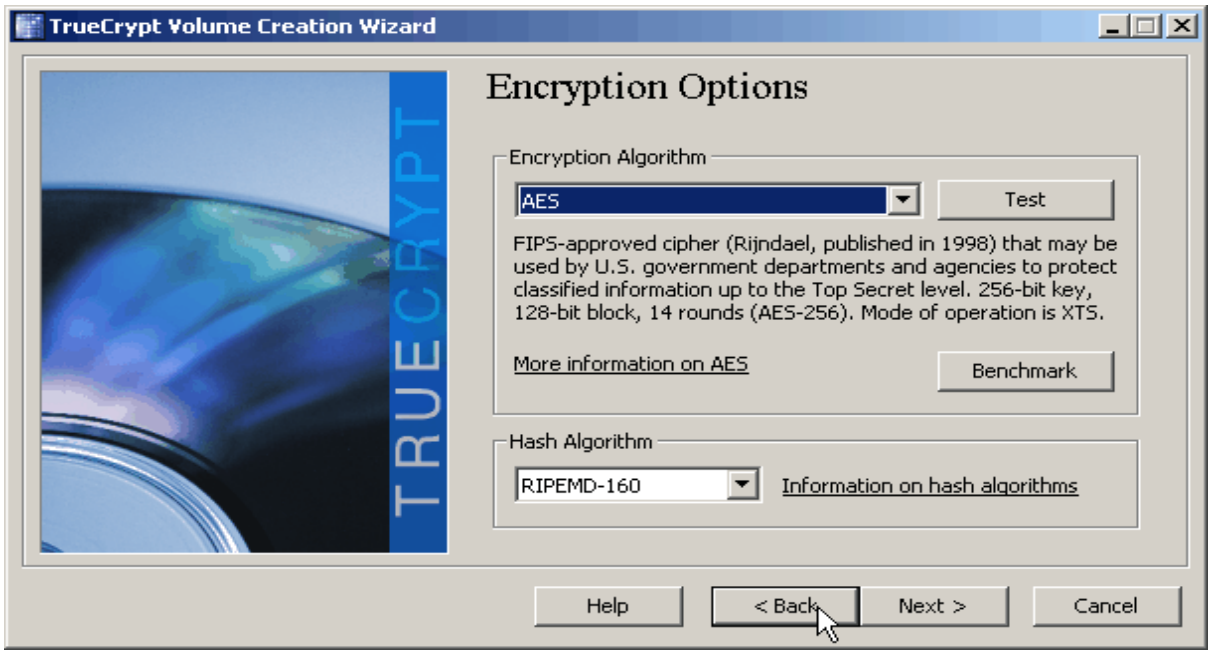
Use the 'Select Device' button to select the device or partition to be encrypted. In this case, the only partition on a USB memory stick has been selected i.e. the full memory stick in this instance. Clicking 'Next' produces the following warning window.

TrueCrypt Volume Creation Wizard
IMPORTANT: We strongly recommend that inexperienced users create a TrueCrypt file container on the selected device/partition, instead of attempting to encrypt the entire device/partition.
When you create a TrueCrypt file container (as opposed to encrypting a device or partition) there is, for example, no risk of destroying a large number of files. Note that a TrueCrypt file container (even though it contains a virtual encrypted disk) is actually just like any normal file. Therefore, it can be, for example, easily renamed, moved, or copied as any normal file. For more information, see the chapter Beginner's Tutorial in the TrueCrypt User Guide.
Are you sure you want to encrypt the entire device/partition?
Yes
No

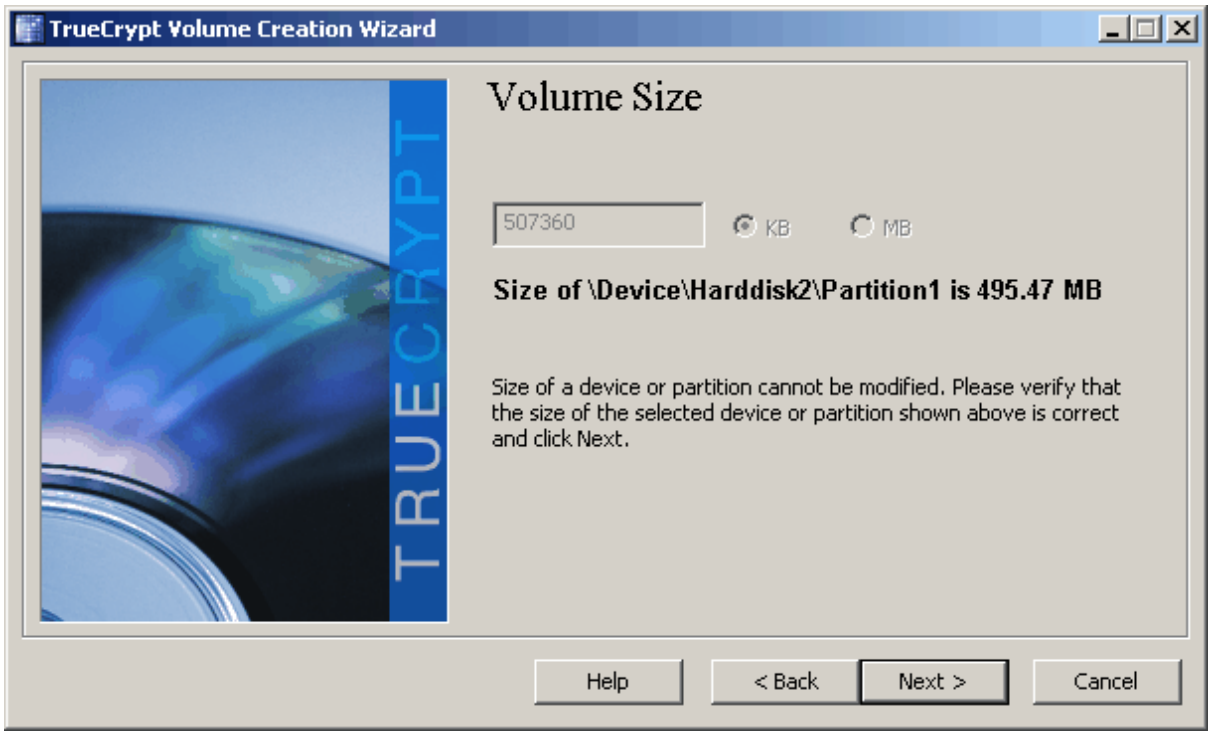
This appears because encrypting a partition can cause the loss of much data, if data preservation has not been planned for. Clicking 'Yes' produces the following error message if the USB device, as opposed to the partition, had been selected in the Volume Location window.


TrueCrypt Volume Creation Wizard
The selected device contains partitions.
Formatting the device might cause system instability and/or data corruption. Please either select a partition on the device, or remove all partitions on the device to enable TrueCrypt to format it safely.
OK

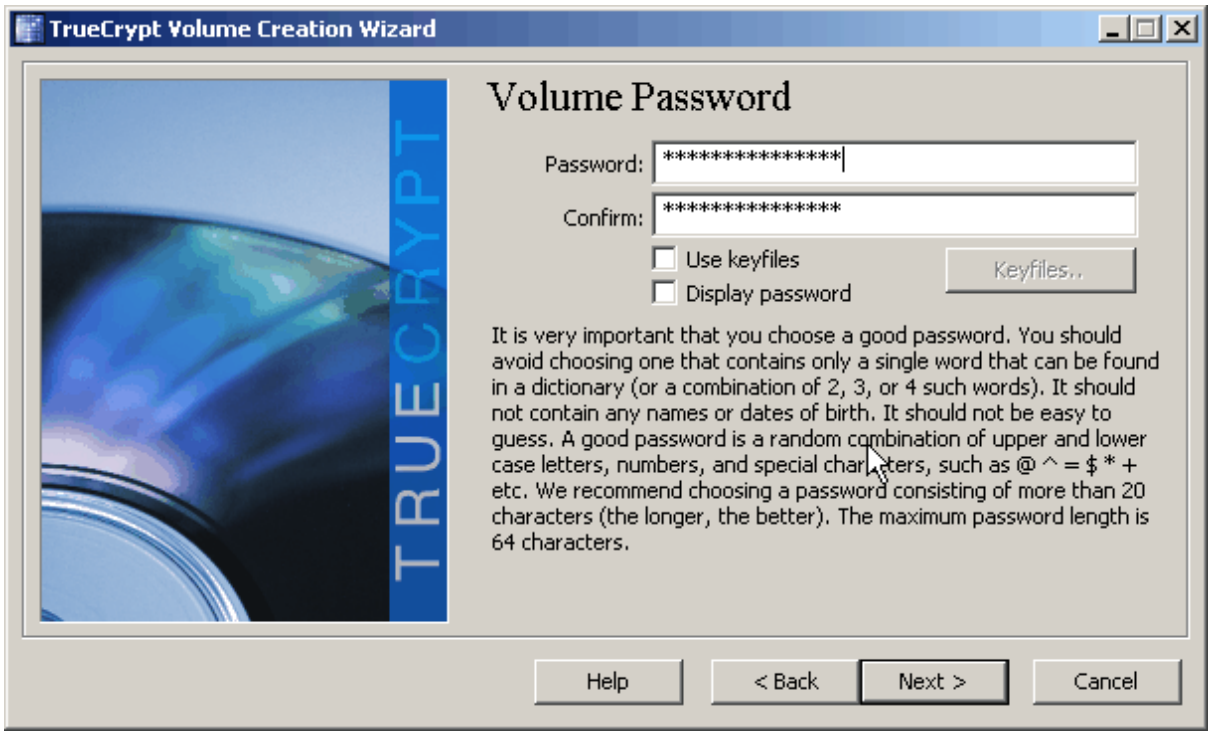
Assuming that the partition had been selected, clicking 'Yes' in the warning window leads to the next window appearing.


TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel

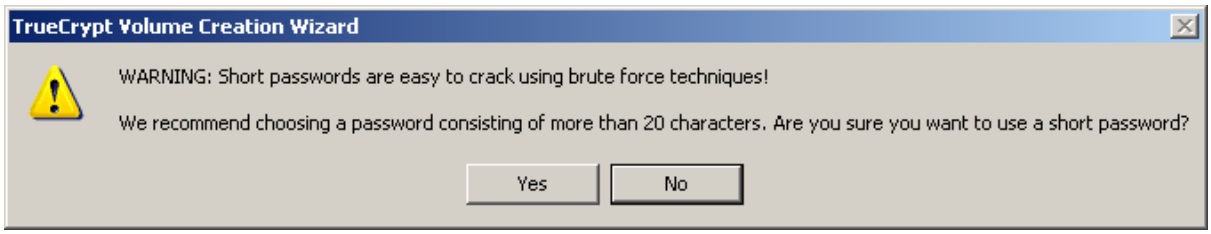
Unless you have good reason for adjusting the encryption and hash algorithms, just click 'Next' to continue.


TrueCrypt Volume Creation Wizard
Volume Size
507360
KB
MB
Size of \Device\Harddisk2\Partition1 is 495.47 MB
Size of a device or partition cannot be modified. Please verify that the size of the selected device or partition shown above is correct and click Next.
TRUECRYPT
Help
< Back
Next >
Cancel

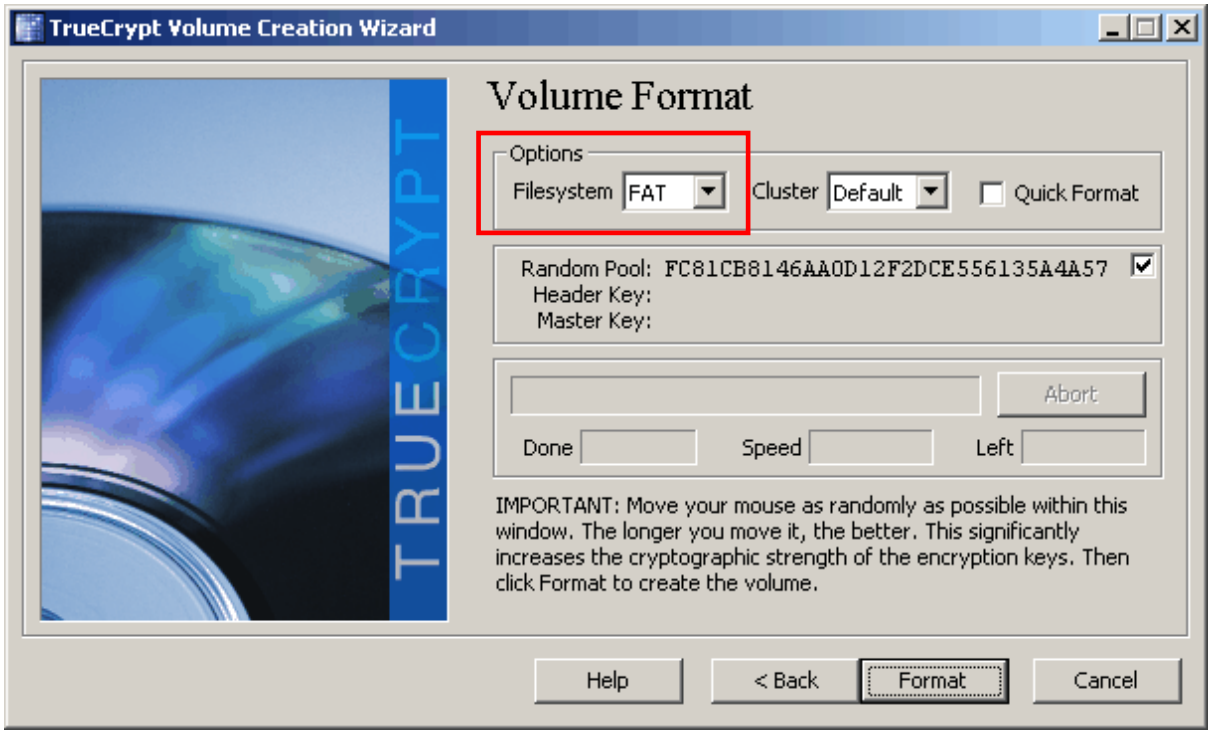
Just verify that the volume size is correct and then click 'Next' to continue.


TrueCrypt Volume Creation Wizard
Volume Password
Password:
Confirm:
Use keyfiles
Keyfiles...
Display password
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.
TRUECRYPT
Help
< Back
Next >
Cancel

Enter the volume password and make a careful note of it. If this password is lost, you will not be able to recover any data stored on the volume. Click 'Next' to proceed. If you use too short a password or phrase, a warning window will appear.


TrueCrypt Volume Creation Wizard
WARNING: Short passwords are easy to crack using brute force techniques!
We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?
Yes
No

After lengthening the password or clicking 'Yes', the next window appears.

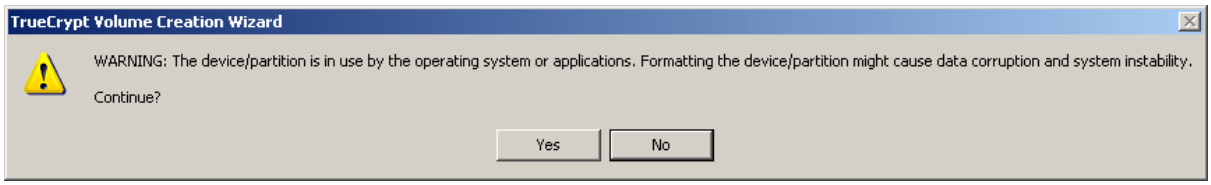



It is better to select NTFS filesystem format in options (red box), instead of FAT. Click the 'Format' button and the following warning appears.

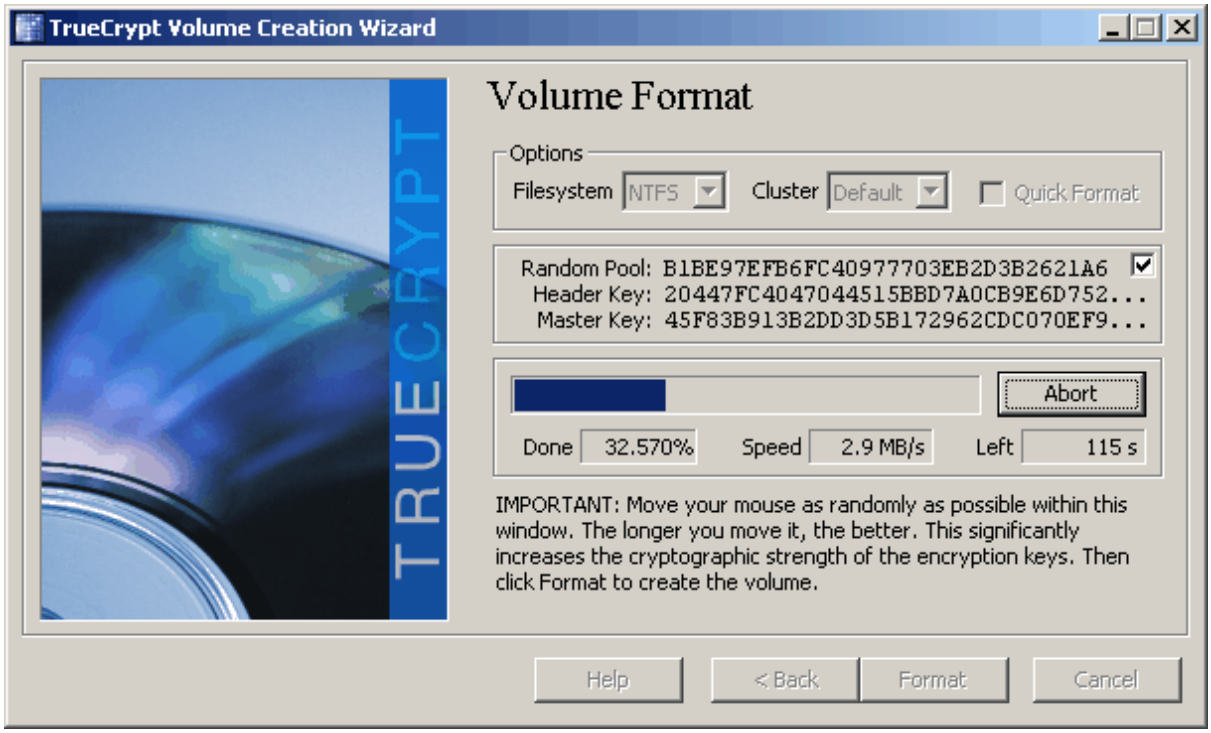
TrueCrypt Volume Creation Wizard
CAUTION: ALL FILES CURRENTLY STORED ON THE SELECTED PARTITION '\Device\Harddisk2\Partition1' (F: 'USBOOT') WILL BE ERASED AND LOST (THEY WILL NOT BE ENCRYPTED)!
Are you sure you want to proceed with format?
Yes
No

If you wish to retain existing data in the partition and it has not been copied elsewhere already, click 'No' to return to the Volume Format window and copy your data to a safe place. Once this has been done, click 'Format' again to continue and click 'Yes' in the window above.

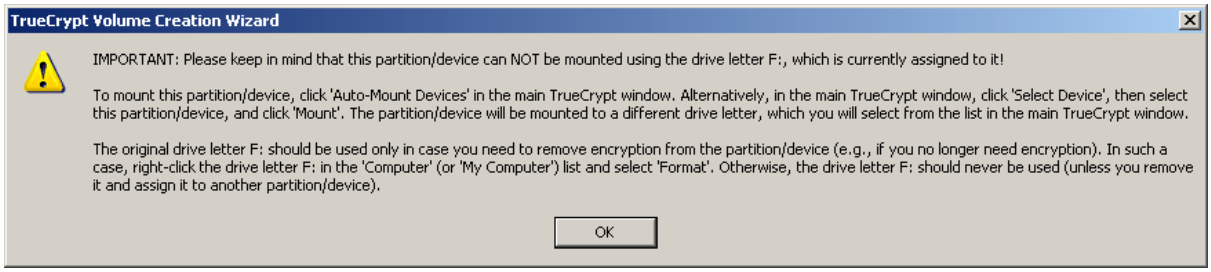
Because a volume is likely to have a drive letter associated with it, the warning window below appears. It is usually safe to ignore it and click 'Yes'.


TrueCrypt Volume Creation Wizard
WARNING: The device/partition is in use by the operating system or applications. Formatting the device/partition might cause data corruption and system instability.
Continue?
Yes
No

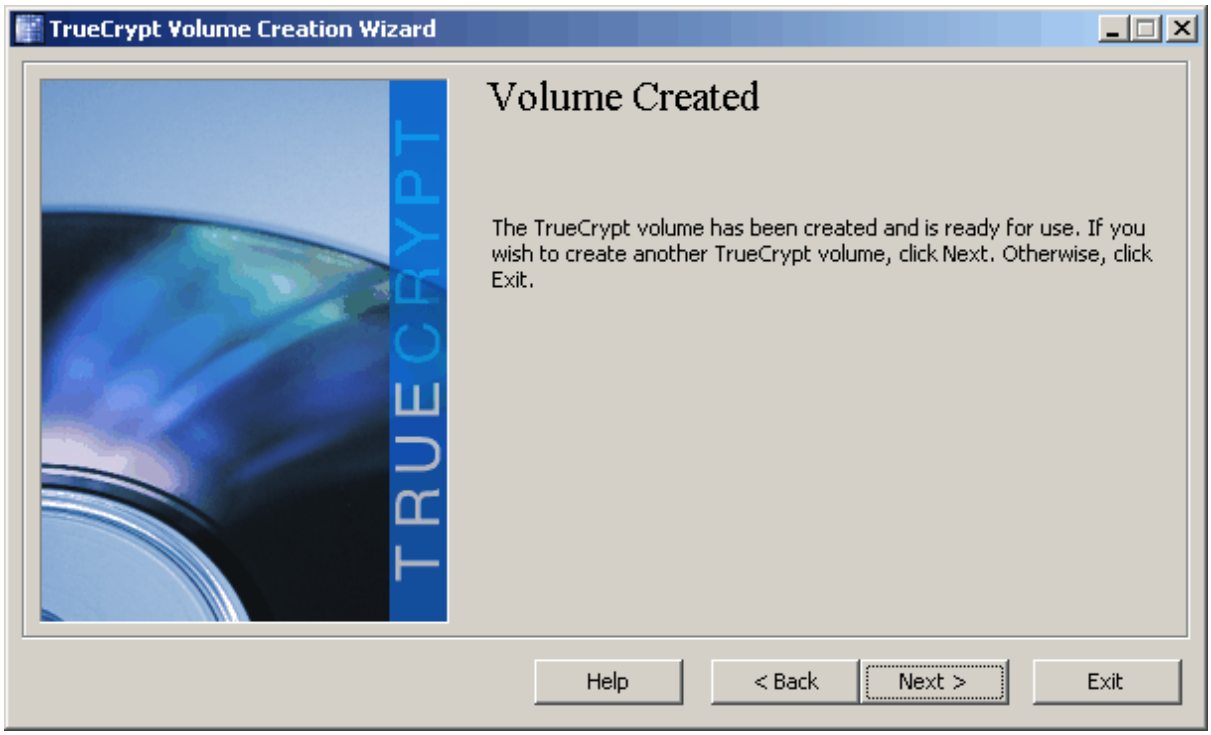
As formatting proceeds, the Volume Format Window will display progress. The 'Abort' button can be used to stop formatting but that will not recover deleted data.




After formatting finishes, a message appears to remind you that the drive letter of the partition is now not usable. It also tells how to mount the newly created encrypted volume.


TrueCrypt Volume Creation Wizard
IMPORTANT: Please keep in mind that this partition/device can NOT be mounted using the drive letter F:, which is currently assigned to it!
To mount this partition/device, click 'Auto-Mount Devices' in the main TrueCrypt window. Alternatively, in the main TrueCrypt window, click 'Select Device', then select this partition/device, and click 'Mount'. The partition/device will be mounted to a different drive letter, which you will select from the list in the main TrueCrypt window.
The original drive letter F: should be used only in case you need to remove encryption from the partition/device (e.g., if you no longer need encryption). In such a case, right-click the drive letter F: in the 'Computer' (or 'My Computer') list and select 'Format'. Otherwise, the drive letter F: should never be used (unless you remove it and assign it to another partition/device).
OK

Click the 'OK' and the final window appears.


TrueCrypt Volume Creation Wizard
Volume Created
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.
TRUECRYPT
Help
< Back
Next >
Exit

Click 'Exit' to finish or 'Next' to create another volume.